修 士 論 文 の 和 文 要 旨

大学院	電気通信学研究科 博士前期課程	情報通信工学専攻
氏名	伏見 和男	学籍番号 0530046
論文題目	効率のよい相手認証に関する研究	

要 旨

あらゆるものがネットワークに接続される「ユビキタス社会」では，従来の人間と機器間だけではなく，機器間の認証が必要になる．このようにサービスの提供に先立ち行われる認証技術の必要性はいっそう高まっている．

この認証の際，利用者を特定するために通常は固定の相手識別子(以後IDと記述)を使用するが，この場合，第三者が利用者の嗜好や行動パターンを把握することが容易となる．つまり，IDからプライバシ情報が漏洩する可能性が高い．またID が固定であることは，悪意のある不正者がサービス提供者のID を使用し，許容量以上のサービス利用要求を行うことで，サービス提供サーバを無力化させてしまうリソース占有攻撃を容易にする．

これらの問題に共通することは，サービス利用者の認証に固定IDを利用する点である．そこでこの問題の対策としては，(1)第三者がIDから利用者を特定することを不可能とすること，(2) 通信を行う二者間のIDはセッション毎に更新すること，(3) 第三者が次のIDを予測することを不可能とすることで問題を解決する「使い捨てID」の活用がある．

使い捨てIDを利用した認証方式としてSIGNAL方式がある．この方式は，使い捨てIDを使用した認証方式という点ではプライバシ漏洩の防止及びリソース占有攻撃対策には効果があるが，処理の過程で秘密鍵，及びべき乗計算を必要し，結果として多くの計算能力を必要とする．また，通信量が増大するなどの問題もある．

そこで本研究では上記の問題点を解決するため，秘密鍵及びべき乗計算を必要としない，使い捨てID を利用した効率のよいリソースの節約が可能な相手認証方式であるDynamic-ID（以後D-ID）方式を提案した．また，計算機上にD-ID方式とSIGNAL方式を実装し，認証に要する時間を計測し，その優位性を確認した．

その結果，D-ID方式がSIGNAL方式に比べ，認証システム全体としては約13倍，方式特有となる認証処理部分に関しては約400倍高速な処理をするという結果を得た．これにより，D-ID方式がリソースの節約が可能な相手認証方式であるということが示せた．